# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.**

# Error correction system for digital signals coded in Reed-Solomon codes.

Patent Number: EP0133137
Publication date: 1985-02-13
Inventor(s): CATREVAUX ALAIN R
Applicant(s): TELEDIFFUSION FSE (FR)
Requested Patent: EP0133137, B1
Application Number: EP19840401597 19840730
Priority Number(s): FR19830012581 19830729
IPC Classification: H03M13/00
EC Classification: H03M13/15P
Equivalents: BR8407000, CA1218461, DE3475253D, DK139585, ES8601520, FI851264, FR2549984, JP60501930T, NO851302, PT78995, WO8500714, YU133684
Cited patent(s): EP0061345; GB2093238

## Abstract

Method for decoding data coded in Reed-Solomon code with correction of errors, wherein the code words are represented by bits forming a polynomial degree (n-1) comprised of m symbols of information and k control symbols with m+k = n-1, the control symbols being formed by words of 2

bits, said words forming the elements of a finite body of Gallois CG (2

) comprising the following steps: (i) dividing a packet of bits to be coded by a code generator polynomial of order k, and as a result the portion of the division provides the m information symbols and the remainder of the division be k control symbols; (ii) calculating the syndromes of the polynomial representative of a code word for certain roots of the code generator polynomial, those syndromes being eight and being related by a system of four linear equations of which the coefficients ( sigma 1 - sigma 4) are the locations of the errors in the code word; and resolving those localizing equations.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication: **0 133 137**
**A1**

(12) # DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt: 84401597.4

(22) Date de dépôt: 30.07.84

(51) Int. Cl.⁴: H 03 M 13/00

(30) Priorité: 29.07.83 FR 8312581

(43) Date de publication de la demande:
13.02.85 Bulletin 85/7

(84) Etats contractants désignés:
AT BE CH DE FR GB IT LI LU NL SE

(71) Demandeur: Etablissement Public de Diffusion dit "Télédiffusion de France"
21-27 rue Barbès
F-92120 Montrouge(FR)

(72) Inventeur: Catrevaux, Alain R.
24, Avenue des Tilleuls
F-94320 Thiais(FR)

(74) Mandataire: Martinet & Lapoux
62, rue des Mathurins
F-75008 Paris(FR)

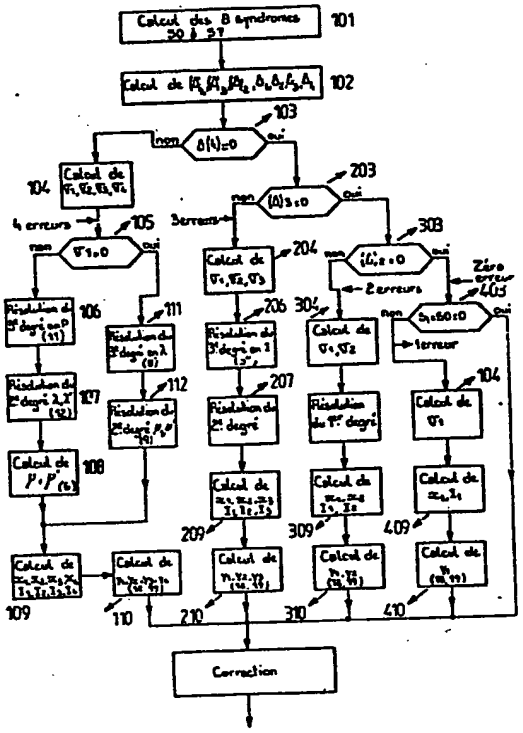
(54) **Système de correction d'erreurs de signaux numériques codés en code de Reed-Solomon.**

(57) Procédé de décodage de données codées en code de Reed-Solomon avec correction d'erreurs dans lequel les mots de code sont représentés par des bits formant un polynôme de degré (n-1) composé de m symboles d'information et k symboles de contrôle avec m+k = n-1, les symboles de contrôle étant formés de mots de 2 bits, lesdits mots constituent les éléments d'un corps fini de Galois CG (2 ) comprenant les stades suivants: (i) diviser un paquet de bits à coder par un polynôme générateur de code d'ordre k, d'où il résulte que le quotient de la division fournit les m symboles d'information et le reste de la division les k symboles de contrôle; (ii) calculer les syndromes du polynôme représentatif d'un mot de code pour certaines des racines du polynôme générateur de code, ces syndromes étant au nombre de huit et étant reliés par un système de quatre équations linéaires dont les coefficients ($\sigma_1 - \sigma_4$) sont les localisations des erreurs dans le mot de code; et résoudre ces équations de localisation.

EP 0 133 137 A1

./...

FIG-3


Calcul des 8 syndromes S0 à S7
101
Calcul de
102
103
non
oui
Calcul de
104
4 erreurs
105
non
oui
Résolution du 2nd degré en D
106
Résolution du 2nd degré en λ
111
Résolution du 2nd degré en
107
112
Calcul de
108
Calcul de
109
Calcul de
110
3erreurs
204
206
207
Calcul de
209
Calcul de
210
2 erreurs
304
Résolution du 1er degré
309
310
Zéro erreur
403
1erreur
Calcul de
409
410
Correction

# SYSTEME DE CORRECTION D'ERREURS DE SIGNAUX NUMERIQUES CODES EN CODE DE REED-SOLOMON

La présente invention concerne une méthode de codage et de décodage de données numériques par un code correcteur d'erreurs ainsi qu'un codeur et un décodeur mettant en oeuvre ladite méthode. Plus précisément, l'invention concerne une méthode de codage et de décodage de données par le code de Reed-Solomon et les codeurs et décodeurs qui appliquent cette méthode.

Le code de Reed-Solomon est décrit par exemple dans l'ouvrage "The Theory of Error-Correcting Codes" par F.J. MacWilliams et N.J.A. Sloane, North Holland Publishing Company, 1981, Chapitre 10.

On rappelle qu'un code de Reed-Solomon dans un corps ou champ fini de Gallois CG(q) est un code de Bose, Chaudhuri, Hocquenhem (BCH) de longueur $N = q-1$.

Les codes BCH sont des codes dont le polynôme générateur est par définition le suivant :

$$G(x) = (x-a^{m_o})\ (x-a^{m_o+1})\ \ldots\ (x-a^{m_o+\delta-2})$$

où $\delta$ est la distance désignée. Avec $\delta-2 = 2t+1$ si t désigne le nombre d'erreurs à corriger.

Les racines de G(x) sont donc les puissances successives d'un élément primitif appartenant à CG (2). Cela veut dire que dans un mot de code :

$$V(x) = y_{n-1}x^{n-1} + \ldots y_{n-1}\ x^{n-i} + \ldots y_o$$

$Y_{n-i}$ a deux valeurs possibles 0 ou 1 ;

et $x^{n-i}$ détermine la position de $y_{n-i}$.

Dans un code de Reed-Solomon, la caractéristique du corps n'est plus 2 mais un entier premier quelconque b donnant lieu à un corps CG ($b^p$). Chaque $y_{n-i}$ n'a plus deux formes possibles mais $q = b^p$ formes. Le coefficient $y_{n-i}$ est un symbole du code.

On définit ainsi des polynômes dont les coefficients sont non plus seulement des entiers 0 ou 1 (base 2) mais des éléments de CG ($b^p$) qui seront exprimés par p éléments binaires.

Par exemple, si $m_o = 0$, $q = 2^3$ et si le polynôme caractéristique qui génère les éléments du corps est égal à $x^3 + x^2 + L$, chaque coefficient va s'exprimer sous la forme d'un mot de 3 bits.

| $a^2$ | a | 1 | |
|---|---|---|---|
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | a |
| 1 | 0 | 0 | $a^2$ |
| 1 | 0 | 1 | $a^3 = 1 + a^2$ |
| 1 | 1 | 1 | $a^4 = a + a^3 = 1 + a + a^2$ |
| 0 | 1 | 1 | $a^5 = a + a^2 + 1 + a^2 = 1 + a$ |
| 1 | 1 | 0 | $a^6 = a + a^2$ |
| 0 | 0 | 1 | $a^7 = a^2 + a^3 = a^2 + a^2 + 1 = 1$ |

On définit alors, comme pour le cas binaire, les racines des polynômes et pour $m_o = 0$, le polynôme générateur de code est :

$$G(x) = (x-1)(x-a) \ldots (x-a^{\delta-2})$$

Le polynôme générateur doit avoir un nombre de racines égal à 2 fois le nombre t d'erreurs à corriger. En effet, la racine a la puissance la plus élevée

$$a^{\delta-2} = a^{2t+1-2} = a^{2t-1}$$

Les racines du polynôme générateur sont donc :

$$1, a, a^2, \ldots a^{2t-1}.$$

Comme on a pris $q = 8$, les mots du code ont une longueur de $N = 7$ symboles. Un code C (7,4) contient quatre symboles d'information et trois symboles de contrôle de chacun trois bits. Le mot de code s'écrit par exemple :

$$\underbrace{(001)\,x^6 + (101)\,x^5 + (000)\,x^4 + (000)\,x^3}_{I(x)} + \underbrace{(011)\,x^2 + 101\,x^1 + (010)\,x^0}_{R(x)}$$

où I(x) désigne les symboles d'information et R(x) les symboles de contrôle constitués par le reste de la division I(x) par G(x).

Une erreur est caractérisée par sa valeur et sa position dans un mot de code donné. Dans le cas d'un code binaire, il suffit de déterminer la position de l'erreur, sa valeur étant obtenue en complémentant la valeur erronée à la position calculée. Donc corriger deux erreurs à l'aide d'un code binaire revient à résoudre un système de deux équations à deux inconnues. Par contre, dans le cas d'un code de Reed-Solomon, un symbole

du code représente un paquet de p éléments binaires. Dans ce cas, deux erreurs sont caractérisées par quatre paramètres, respectivement leurs deux valeurs et positions.

L'invention tant en ce qui concerne la méthode de codage que le codeur et le décodeur de code Reed-Solomon, va être maintenant décrite en détail en relation avec les dessins annexés, dans lesquels :

- la Fig. 1 représente sous la forme d'un diagramme de blocs le codeur pour code de Reed-Solomon conforme à l'invention ;
- la Fig. 2 représente le décodeur pour code de Reed-Solomon conforme à l'invention ; et
- la Fig. 3 représente l'algorithme de décodage.

1 - CODAGE

Ainsi qu'on l'a dit dans l'entrée en matière, les symboles du code sont des éléments du champ fini de $2^p$ éléments. Chaque symbole du code comporte p éléments binaires. Les symboles de contrôle sont obtenus en divisant le message informationnel I(x) par le polynôme générateur G(x).

Le code comporte m symboles d'information et k symboles de contrôle. On désigne le code par C(m + k, m). Une méthode de codage bien connue consiste à prémultiplier I(x) par $x^k$, k étant le degré le plus élevé du polynôme générateur et à diviser le produit ainsi obtenu par G(x), soit :

$$\frac{x^k\, I(x)}{G(x)}$$

où G(x) a la forme polynomiale précédemment indiquée avec $k = m + \delta - 1$.

Le code décrit est un code C(255, 247) avec $2^p = 2^8$,

d'où $G(x) = x^8 + Ax^7 + Bx^6 + Cx^5 + Dx^4 + Ex^3 + Fx^2 + Gx + H$ (20)

Les coefficients A, B, C, D, E, F, G et H sont des mots de huit bits.

Lorsque le premier symbole apparaît à l'entrée du système, les restes partiels précédents sont nuls. Soit $S_1$, ce premier symbole. Le circuit 2 stocke temporairement $S_1$ le temps que le circuit 3 fournisse le résultat de la multiplication $S_1$ par chacun des termes du polynôme générateur. Ces restes partiels sont stockés dans le circuit 1 dans un ordre qui est une caractéristique du système.

Quand le deuxième symbole $S_2$ se présente à l'entrée du système, on additionne modulo 2, $S_2$ avec le reste partiel précédent de degré le plus élevé. Le résultat de cette opération est stocké dans 2. Ensuite, le circuit 3 effectue les multiplications avec les restes partiels précédents et le processus continue, jusqu'à ce que le 247ième symbole d'information soit rentré dans le système.

Le circuit 1 est une mémoire vive de k mots de p bits.

Les circuits 2 et 3 sont des unités de stockage de p bits.

Le circuit 4 est un additionneur modulo 2 de p bits.

Quant au circuit 5, il est constitué d'une table inaltérable qui, adressée par $(S_i + R_{pi})$ fournit respectivement les produits de $(S_i + R_{pi})$ par chacun des coefficients de G(x).

Avec $S_i$ désignant le symbole informationnel d'ordre i et $R_{pi}$, le reste partiel d'ordre i de même degré que $S_i$.

Lorsque tous les symboles d'information constituant I(x) sont entrés dans le système, le circuit 1 contient les 8 symboles de contrôle rangés dans un certain ordre. Symboles qu'il suffit d'appeler en ligne à la suite de $x^k$ I(x) pour finir de constituer le mot de code.

2 - DECODAGE

La méthode de décodage conforme à l'invention utilise un système unique pour calculer :

- les syndromes d'erreurs ;
- les coefficients du polynôme localisateur d'erreurs ;
- les racines du polynôme localisateur d'erreurs ;
- les diagrammes d'erreurs correspondant aux positions d'erreur calculées ;
- les corrections.

CALCUL RELATIF A LA CORRECTION DE QUATRE ERREURS. CALCUL DES SYNDROMES

V(x) étant un mot de code, s'il y a des erreurs, il s'écrit $V'(x) = V(x) + E(x)$.

E(x) étant la configuration d'erreurs apparue au cours de la transmission.

Afin de déceler les erreurs à la réception, il faut soit vérifier que les mots reçus sont divisibles ou non par le polynôme générateur,

soit vérifier que chaque mot de code admet pour racines les racines du polynôme générateur. Cette deuxième solution est celle utilisée pour le décodage de la présente invention.

Un mot de code V(x) s'écrit sous la forme d'un polynôme de la manière suivante, ainsi qu'on l'a vu précédemment

$$V(x) = y_{n-1}\, x^{n-1} + y_{n-2}\, x^{n-2} + \ldots y_{n-i}\, x^{n-i} + \ldots + y_o\, x^o \qquad (1)$$

Si V(x) admet $a^j$ pour racine, cela s'écrit :

$$V(a^j) = y_{n-i}(a^j)^{n-1} + y_{n-2}(a^j)^{n-2} + \ldots + y_{n-i}(a^j)^{n-i} + \ldots + y_o(a^j)^o$$

$$V(a^j) = \sum_{i=n-1}^{i=o} y_i (a^j)^i = S_o \qquad (2)$$

S'il y a une erreur, on reçoit non plus le mot de code $V(a^j)$ mais le mot de code

$$V'(a^j) = V(a^j) + E(a^j) = S_j$$

puisque $V(a^j) = 0$.

$S_j$ est le syndrome d'erreur d'ordre j, il faut calculer les syndromes $S_j$ avant de pouvoir déterminer la position et la valeur des erreurs.

Si on reçoit un mot erroné, il y a donc une certaines configuration d'erreurs E(x) dont chacune peut être repérée par un couple $x_i$, $y_i$ (position et valeur).

## CALCUL DES COEFFICIENTS DU POLYNOME LOCALISATEUR D'ERREURS A PARTIR DES SYNDROMES

Si on veut corriger t erreurs, le polynôme localisateur d'erreurs s'écrit :

$$X_i^t + \sigma_1 X_I^{t-1} + \sigma_2 X_I^{t-2} + \ldots \sigma_j X_I^{t-j} + \ldots \sigma_t = 0 \qquad (3)$$

Les coefficients $\sigma_1$, $\sigma_2$ ... $\sigma_t$ sont obtenus en résolvant le système suivant :

$$S_t + \sigma_1 S_{t-1} + \sigma_2 S_{t-2} + \ldots \sigma_j S_{t-j} + \ldots + \sigma_t S_o = 0$$

$$S_{t+1} + \sigma_1 S_t + \sigma_2 S_{t-1} + \ldots\ldots\ldots\ldots + \sigma_t S_1 = 0$$

$$S_{2t-1} + \sigma_1 S_{2t-2} + \ldots\ldots\ldots\ldots\ldots\ldots + \sigma_t S_{t-1} = 0$$

Soit $\Delta$ le déterminant principal du système, il est égal à :

$$\Delta = \begin{vmatrix} S_{t-1} & S_{t-2} \ldots\ldots S_{t-i} \ldots\ldots\ldots S_o \\ S_t & S_{t-1} \ldots\ldots S_{t-i+1} \ldots\ldots\ldots S_1 \\ \vdots & \\ S_{2t-2} & S_{2t-3} \ldots\ldots S_{2t-i-1} \ldots\ldots\ldots S_{t-1} \end{vmatrix}$$

En appliquant les règles sur la résolution des systèmes d'équation linéaires, il vient : $\sigma_i = \Delta_i / \Delta$ où

$$\Delta_i = \begin{vmatrix} S_{t-1} & S_{t-2} \ldots\ldots S_t \ldots\ldots\ldots\ldots S_o \\ S_t & S_{t-1} \ldots\ldots S_{t+1} \ldots\ldots\ldots\ldots S_i \\ \vdots & \vdots \quad\quad \vdots \quad\quad\quad\quad \vdots \\ S_{2t-2} & S_{2t-3} \quad\quad S_{2t-1} \quad\quad\quad\quad S_{t-1} \end{vmatrix}$$

Les coefficients de polynôme localisateur d'erreurs ont donc pour valeurs respectives les valeurs suivantes :

$$\sigma_t = \Delta_t / \Delta \ldots\ldots \sigma_i = \Delta_i / \Delta \ldots\ldots \sigma_1 = \Delta_1 / \Delta \qquad (4)$$

CALCUL DES RACINES DU POLYNOME LOCALISATEUR D'ERREURS

L'équation (3) n'étant résoluble que si elle est au plus du quatrième degré, le système peut corriger jusqu'à quatre erreurs. Les positions des quatre erreurs sont donc solutions de :

$$X^4 + \sigma_1 X^3 + \sigma_2 X^2 + \sigma_3 X + \sigma_4 = 0 \qquad (3')$$

Cette équation peut aussi se mettre sous la forme bicarrée :

$$(X^2 + \lambda X + \mu)\ (X^2 + \lambda' X + \mu') = 0 \qquad (5)$$

Avec :

$$\left.\begin{aligned} \sigma_1 &= \lambda + \lambda' \\ \sigma_2 &= \mu + \mu' + \lambda\lambda' \\ \sigma_3 &= \lambda\mu' + \lambda'\mu \\ \sigma_4 &= \mu\mu' \end{aligned}\right\} \qquad (6)$$

Pour localiser les erreurs, il suffit de déterminer les valeurs de $\lambda$, $\lambda'$, $\mu$ et $\mu'$, puis les racines de chacune des équations du second degré. Pour résoudre le système (6), deux cas se présentent suivant que $\sigma_1$ est nul ou non nul, en effet :

Le système (6) devient pour $\sigma_1 = 0$

$$\left.\begin{aligned} \lambda + \lambda' &= 0 \\ \sigma_2 &= \mu + \mu' + \lambda^2 \\ \sigma_3 &= \lambda\ (\mu + \mu') \\ \sigma_4 &= \mu\mu' \end{aligned}\right\} \qquad (7)$$

d'où :

$$\left.\begin{aligned} \sigma_2 &= \frac{\sigma_3}{\lambda} + \lambda^2 \\ \lambda^3 &+ \sigma_2 \lambda + \sigma_3 = 0 \end{aligned}\right\} \qquad (8)$$

Cette équation est du troisième degré en $\lambda$ et fournit une racine $\lambda_1$. Les quantités $\mu$ et $\mu'$ sont solution d'une équation du second degré, sachant que :

$$\mu + \mu' = \sigma_3 / \lambda_1$$

$$\mu\mu' = \sigma_4$$

$\mu$ et $\mu'$ sont racines de

$$\mu^2 + (\sigma_3/\lambda_1)\ \mu + \sigma_4 = 0 \qquad (9)$$

Pour $\sigma_1 \neq 0$, on a en posant

$$\sigma_1 = \lambda + \lambda'$$

$$\rho = \lambda\lambda' \qquad (10)$$

On aboutit à une équation du troisième degré en $\rho$, soit :

$$\rho^3 + (\sigma_1 \sigma_3 + \sigma_2^2)\ \rho + \sigma_1^2 \sigma_4 + \sigma_3^2 + \sigma_1 \sigma_2 \sigma_3 = 0 \qquad (11)$$

On en tire une racine $\rho_1$ par exemple. D'où $\lambda$ et $\lambda'$ sont solution d'une équation du second degré, soit :

$$\lambda^2 + \sigma_1 \lambda + \rho_1 = 0 \qquad (12)$$

Le système (6) permet alors de déduire les valeurs de $\mu$ et de $\mu'$.

RESOLUTION D'UNE EQUATION DU TROISIEME DEGRE DE TYPE (8) ou (11)

Ces deux équations sont de la forme :

$$y^3 + \nu y + \tau = 0 \qquad (13)$$

Cette équation peut se mettre sous la forme canonique (coefficient de y égal à l'unité) en posant :

$$z = y/\nu^{1/2}$$

et

$$Q = \tau/\nu^{3/2}$$

ce qui donne :

$$z^3 + z + Q = 0 \qquad (14)$$

Si p est pair, deux cas se présentent pour trouver une racine cubique dans le corps $CG(2^p)$.

1) Si $\nu = 0$

L'équation (13) devient :

$y_3 + \tau = 0$ est donné par une table

$$y^3 = \tau^{1/3}$$

Ensuite :

$$y_1 + y_2 + y_3 = 0$$

$$y_1 y_2 y_3 = \tau$$

$y_1$ et $y_2$ sont alors solution de :

$$y^2 + y_3 y + \tau/y_3 = 0 \qquad (15)$$

Equation qui se met sous la forme canonique suivante :

$$Y^2 + Y + R = 0 \qquad (16)$$

avec $Y = y/y_3$ $\qquad R = \tau/y_3^3 = 1$

2) Si $\nu \neq 0$, il faut alors résoudre l'équation (14). $z_3$ est obtenu par une table adressée par Q. Les racines $z_1$ et $z_2$ sont obtenues par une méthode identique à celle qu'on vient de voir pour $\nu = 0$ et $R \neq 1$.

La Fig. 3 représente l'algorithme de décodage.

Le nombre d'erreurs que l'on s'impose de corriger est de quatre, trois ou deux.

La phase 101 représente le calcul des syndromes qui dans notre cas, seront au nombre de 8, $S_7$ à $S_0$. La phase 102 représente le calcul de $(\Delta)_4$, $(\Delta)_3$, $(\Delta)_2$, déterminant principal dans le cas de 4, 3 ou 2 erreurs, ainsi que celui de $\Delta_i$, i variant de 1 à 4, soit $\Delta = \Delta_1$, $\Delta_2$, $\Delta_3$, $\Delta_4$.

Si $(\Delta_4)$ est différent de zéro (phase 103), on en déduit qu'il y a 4 erreurs, et on va vers la phase 104 où l'on calcule $\sigma_1$, $\sigma_2$, $\sigma_3$, $\sigma_4$, définis par les équations (4).

Si $\sigma_1 \neq 0$ (phase 105), on passe à la phase 106 de calcul des racines de l'équation en $p^3$ (équation (11)), puis à la phase 107 de calcul des racines $\lambda$, $\lambda'$ de l'équation (12), enfin à la phase 108 de calcul des $\mu$ et $\mu'$ par les équations (6).

On passe ensuite à la résolution de l'équation (5) (phase 109), ce qui donne $X_1$, $X_2$, $X_3$, $X_4$ et on déduit l'adresse de l'erreur à l'aide de la formule (17). Enfin, phase 110, on calcule $\gamma_1$ à $\gamma_4$ par la formule (18).

Si (phase 105), on a $\sigma_1 = 0$, les phases (106-108) sont remplacées par les phases (111-112) qui correspondent respectivement à la résolution de l'équation en $\lambda^3$ (équation (8)) et à la résolution de l'équation en $\mu^2$ (équation (9)).

L'algorithme de la Fig. 3 représente également les phases de décodage dans le cas de la correction de trois erreurs et de deux erreurs. Dans ces deux cas, l'équation (3') devient :

trois erreurs :

$$X^3 + \sigma_1 X^2 + \sigma_2 X + \sigma_3 = 0 \qquad (3'')$$

deux erreurs :

$$X^2 + \sigma_1 X + \sigma_2 = 0 \qquad (3''')$$

L'équation (3") peut être mise sous la forme canonique et une des racines est obtenue par la formule de Cardan (phase (206)). Les deux autres racines sont obtenues en résolvant une équation du second degré en X (phase 207).

On voit sur la Fig. 3 qu'il y a équivalence entre les phases ayant pour numéros de centaines 1, 2, 3, 4 et les mêmes numéros d'unités et de dizaines.

Dans tous les cas de figures à la valeur des coefficients près, on est ramené à la résolution d'une équation du troisième degré ou du deuxième degré mise sous forme canonique.

La position effective des erreurs est déterminée de la façon suivante :

Sachant que $X_i$ est de forme $X_i = a^{ji}$ ($a^{ji}$ étant un élément CG ($2^p$)), $j_i$ caractérise la position de l'erreur, d'où :

$$j_i = \mathrm{Log}_a (X_i) \qquad (17)$$

La détermination des $X_i$ permet alors de calculer les diagrammes d'erreurs $y_i$ correspondants.

$$\left.\begin{aligned} S_0 &= Y_1 + Y_2 + Y_3 + Y_4 \\ S_1 &= Y_1 X_1 + Y_2 X_2 + Y_3 X_3 + Y_4 X_4 \\ S_2 &= Y_1 X_1^2 + Y_2 X_2^2 + Y_3 X_3^2 + Y_4 X_4^2 \\ S_4 &= Y_1 X_1^3 + Y_2 X_2^3 + Y_3 X_3^3 + Y_4 X_4^3 \end{aligned}\right) \qquad (18)$$

$$D = \begin{vmatrix} 1 & 1 & 1 & 1 \\ X_1 & X_2 & X_3 & X_4 \\ X_1^2 & X_2^2 & X_3^2 & X_4^2 \\ X_1^3 & X_2^3 & X_3^3 & X_4^3 \end{vmatrix}$$

$$D_{y1} = \begin{vmatrix} S_o & 1 & 1 & 1 \\ S_1 & X_2 & X_3 & X_4 \\ S_2 & X_2^2 & X_3^2 & X_4^2 \\ S_3 & X_2^3 & X_3^3 & X_4^3 \end{vmatrix}$$

$$D_{y2} = \begin{vmatrix} 1 & S_o & 1 & 1 \\ X_1 & S_1 & X_3 & X_4 \\ X_1^2 & S_2 & X_3^2 & X_4^2 \\ X_1^3 & S_3 & X_3^3 & X_4^3 \end{vmatrix}$$

$$D_{y3} = \begin{vmatrix} 1 & 1 & S_o & 1 \\ X_1 & X_2 & S_1 & X_4 \\ X_1^2 & X_2^2 & S_2 & X_4^2 \\ X_1^3 & X_2^3 & S_3^3 & X_4^3 \end{vmatrix}$$

$$D_{y4} = \begin{vmatrix} 1 & 1 & 1 & S_0 \\ X_1 & X_2 & X_3 & S_1 \\ X_1^2 & X_2^2 & X_3^2 & S_2 \\ X_1^3 & X_2^3 & X_3^3 & S_3 \end{vmatrix}$$

D'où on tire

$$Y_1 = \frac{D_{y1}}{D} \quad ; \quad Y_2 = \frac{D_{y2}}{D} \; ; \; Y_3 = \frac{D_{y3}}{D} \; ; \quad Y_4 = \frac{D_{y4}}{D} \qquad (19)$$

En se référant à la Fig. 2, au fur et à mesure de l'arrivée des symboles, le décodeur calcule $S_j$ conformément à l'équation (2) pour une valeur de j donnée. Cette opération est réalisée autant de fois que G(x) a de racines.

Le circuit 11 calcule pour un symbole de l'ordre $\ell$ $y_\ell (a^j)^\ell$ pour une racine $x_j = a^j$.

Ce résultat est alors stocké temporairement dans le circuit 12.

Le décodeur appelle la somme des $(n-\ell)$ termes précédents, stockée dans le circuit 10, le circuit 11 étant transparent. Le circuit 13 effectue la somme :

$$\sum_{i=n-1}^{\ell-1} y_i (a^j)^i + y_\ell (a^j)^\ell$$

Le calcul de cette opération transite à travers l'unité de stockage 14 et le circuit 15 qui est transparent pour être stocké dans le circuit 10 jusqu'à l'arrivée du symbole suivant et l'opération décrite se renouvelle jusqu'à l'arrivée du dernier symbole. Les différents syndromes sont stockés dans le circuit 10.

Le décodeur est formé de trois unités de stockage :

- le circuit 10 qui est une mémoire vive de u mots de p bits, u étant une caractéristique du système,
- les circuits 12 et 14 qui sont des unités de stockage de p bits.

Un circuit 13 qui, lors du calcul des syndromes, fonctionne en additionneur modulo 2.

. Un circuit 11 qui est une table dont une zone réservée multiplie le symbole présent à son entrée par les racines du polynôme générateur dans un ordre que le système définit à l'avance.

Un circuit 15 qui est une table dont on utilise une zone transparente lors de cette opération.

Les opérations nécessaires pour calculer les différents déterminants sont la multiplication et l'addition modulo 2.

La multiplication de deux éléments du champ d'extension CG ($2^p$) est remplacée par l'addition modulo ($2^p$-1) des logarithmes à base a de ces deux nombres, a étant un élément primitif du champ CG ($2^p$).

## CAS DE MULTIPLICATION

La valeur d'un syndrome stocké dans le circuit 10 transite dans le circuit 11 qui en donne logarithme. Ce résultat est stocké dans le circuit 12. En utilisant le même processus, on calcule par exemple le logarithme d'un autre syndrome. A ce moment, les sorties des circuits 11 et 12 attaquent le circuit 13 fonctionnant dans ce cas bien précis en additionneur modulo ($2^p$-1). Le résultat de l'addition des deux logarithmes est stocké dans le circuit 14. A cet instant, le circuit 15 fournit l'antilogarithme du résultat issu de 14, résultat qui prend place dans une zone réservée du circuit 10.

## CAS DE L'ADDITION

Dans ce cas, les circuits 11 et 15 sont transparents et le circuit 13 fonctionne en additionneur modulo 2.

Les coefficients $\sigma_1$, $\sigma_2$ ..... $\sigma_i$ ..... $\sigma_t$ calculés par la méthode ci-dessus sont stockés dans les zones bien définies du circuit 10.

Exemple

Soit :

$$x^8 + x^4 + x^3 + x^2 + 1$$

le polynôme caractéristique qui peut se mettre sous la forme d'un polynôme générateur de code

$$G(x) = (x-1)\ (x-a)\ \ldots\ (x-a^7)$$

Comme ainsi qu'on l'a vu, il faut que le polynôme générateur ait un nombre de racine double du nombre d'erreurs à corriger, et comme il y a ici huit racines, on peut corriger quatre erreurs. Il y a donc huit syndromes $S_0$ à $S_7$ et ces syndromes sont calculés en remplaçant $a^j$ par successivement 1, a, $a^2$, $a^3$, $a^4$, $a^5$, $a^6$, $a^7$ et en faisant $n-1 = 255$.

On suppose que les syndromes aient les valeurs suivantes :

$$S_0 = a^3$$
$$S_1 = a^5$$
$$S_2 = a^7$$
$$S_3 = a^9$$
$$S_4 = a^{11}$$
$$S_5 = a^{13}$$
$$S_6 = a^{15}$$
$$S_7 = a^{17}$$

On suppose en outre qu'il y ait une erreur ayant pour position $a^2$ et pour valeur $a^3$ où $a^2$ et $a^3$ sont des éléments du corps de Gallois $CG(2^8)$.

Le déterminant principal $\Delta$ qui permet la résolution des inconnues $\sigma_1$ à $\sigma_4$ (déterminant qui est d'ordre 4 pour quatre erreurs) s'écrit :

$$\Delta(4) = \begin{vmatrix} S_3 & S_2 & S_1 & S_0 \\ S_4 & S_3 & S_2 & S_1 \\ S_5 & S_4 & S_3 & S_2 \\ S_6 & S_5 & S_4 & S_3 \end{vmatrix} = 0$$

Ce déterminant est nul. Il y a donc au plus trois erreurs. On forme alors le déterminant principal.

$$\Delta(3) = \begin{vmatrix} S_3 & S_2 & S_1 \\ S_4 & S_3 & S_2 \\ S_5 & S_4 & S_3 \end{vmatrix} = 0$$

Ce déterminant est nul. Il y a donc au plus deux erreurs. On forme alors le déterminant principal.

$$\Delta(2) = \begin{vmatrix} S_3 & S_2 \\ S_4 & S_3 \end{vmatrix} = 0$$

Ce déterminant est nul. Il y a donc une seule erreur. On forme alors

$$\Delta(1) = |S_3| = S_3$$

et le déterminant

$$\Delta_1 = |S_4| = S_4$$

On a alors (équation (4))

$$\sigma_1 = \Delta_1 / \Delta(1) = S_4 / S_3 = a^{11} / a^9 = a^2.$$

L'équation (3') se réduit à

$$X + \sigma_1 = 0$$

d'où $X = \sigma_1 = a^2$

ce qui vérifie l'hypothèse faite pour la position de l'erreur.

L'erreur corrigée est la quantité $y_1$ qui est calculée par l'équation (2). On trouve :

$$y_1 = S_o = a^3$$

REVENDICATIONS

1 - Procédé de décodage de données codées en code de Reed-Solomon avec correction d'erreurs dans lequel les mots de code sont représentés par des bits formant un polynôme de degré (n-1) composé de m symboles d'information et k symboles de contrôle avec m+k = n-1, les symboles de contrôle étant formés de mots de $2^p$ bits, lesdits mots constituent les éléments d'un corps fini de Gallois CG ($2^p$) comprenant les stades suivants :

diviser un paquet de bits à coder par un polynôme générateur de code d'ordre k, d'où il résulte que le quotient de la division fournit les m symboles d'information et le reste de la division les k symboles de contrôle ;

calculer les syndromes du polynôme représentatif d'un mot de code pour certaines des racines du polynôme générateur de code, ces syndromes étant au nombre de huit et étant reliés par un système de quatre équations linéaires dont les coefficients sont les localisations des erreurs dans le mot de code ;

caractérisé en ce qu'on forme le déterminant $\Delta(4)$ dudit système de quatre équations linéaires, et s'il est nul le déterminant $\Delta(3)$ du système de trois équations, et s'il est nul le déterminant $\Delta(2)$ du système de deux équations, et s'il est nul le déterminant $\Delta(1)$ d'une équation unique, le nombre d'erreurs étant de 4, 3, 2 ou 1 selon que respectivement les déterminants $\Delta(4)$, $\Delta(3)$, $\Delta(2)$, $\Delta(1)$ sont nuls ;

et la correction de l'erreur ou des erreurs aux localisations trouvées en résolvant un système d'équations donnant les valeurs des syndromes auxdites localisations.

2 - Système de codage en code de Reed-Solomon permettant d'effectuer le calcul des symboles de contrôle à adjoindre aux symboles d'information, caractérisé en ce qu'il comporte une table (5), trois unités de stockage (1, 2, 3) et un additionneur modulo 2 (4), le tout permettant d'effectuer des multiplications d'une part et d'additionner modulo 2

des termes de degrés identiques, de les stocker dans une unité (1) telle qu'on puisse les reconnaître à chaque étape de la division d'autre part, ledit système du codage permettant de calculer des symboles de contrôle des codes de Reed-Solomon dont les symboles sont dans un champ fini CG ($2^p$), p pouvant avoir une valeur quelconque.

3 - Système de calcul des syndromes d'erreurs dans un code de Reed-Solomon permettant de calculer k syndromes d'erreurs, caractérisé en ce qu'il comprend trois unités de stockage (10, 12, 14), le circuit (10) étant une mémoire vive de u mots de p bits, u étant une caractéristique du système, les circuits (12) et (14) étant des unités de stockage de p éléments binaires, un circuit (13) qui lors du calcul des syndromes, fonctionne en additionneur modulo 2, un circuit (11) qui est une table dont une zone réservée multiplie le symbole présent à son entrée par les racines du polynôme générateur dans un ordre que le système définit à l'avance, et un circuit (15) qui est une table dont on utilise une zone transparente lors de cette opération.

4 - Système conforme à la revendication 2 permettant en outre de calculer les t coefficients de p bits du polynôme localisateur d'erreurs, caractérisé en ce qu'un circuit (16) teste successivement la valeur des déterminants $(\Delta)_4, (\Delta)_3, (\Delta)_2 \ldots (\Delta)_1$ jusqu'à l'instant où il trouve $(\Delta)_i \neq 0$ et à ce moment et suivant la valeur de i, le circuit (16) délivre une information qui indique le nombre d'erreurs rencontrées d'une part et permet au système de calculer les coefficients $\sigma_i$ correspondant au nombre d'erreurs à corriger d'autre part.

5 - Système conforme aux revendications 2 et 3, caractérisé en ce que le circuit (10) détecte le type d'opération à effectuer afin de l'indiquer au circuit (13) qui, suivant le cas, se positionne en additionneur modulo 2 ou modulo $(2^{p-1})$ et que les circuits (11) et (15) sont des tables dont certaines zones fournissent respectivement $\text{Log}_a\ (a^i)$ et $\text{Log}_a^{-1}\ (a^i)$, $a^i$ étant un élément de CG ($2^p$), et qu'en outre, le système possède au travers du circuit (16) un détecteur de configurations d'opérations interdites telles que $\text{Log}_a\ (0)$, le système permet de réaliser le calcul $\sigma_1$ à $\sigma_4$.

6 - Système conforme aux revendications 2, 3 et 4, caractérisé en ce que le circuit (16) permet, à la suite de tests successifs, de déterminer le nombre d'erreurs apparues, et que dans le cas où il y a quatre erreurs, le système en calcule les positions à partir d'équations du troisième degré mises sous forme canonique, et qu'en outre, le circuit (15) est constitué de manière telle qu'il détecte les cas où l'équation du troisième degré n'a pas de solutions afin d'adapter la procédure de poursuite des calculs.

7 - Système conforme aux revendications 2, 3, 4 et 5, caractérisé en ce que le circuit (15) est une table inaltérable dont certaines zones fournissent les racines d'une équation du troisième et du second degré mises sous forme canonique.

8 - Système conforme aux revendications 2 à 6, caractérisé en ce que la conjonction des circuits (15) et (16) évite d'ajouter des erreurs supplémentaires lorsqu'il apparaît plus de quatre erreurs.

9 - Système conforme aux revendications 2 à 7, caractérisé en ce que le circuit (10) à partir des informations qui y sont stockées, permet de corriger les symboles erronés aux positions déterminées par le calcul.

Martinet & Lapoux

0136137

62, RUE DES MATHURINS 75008 PARIS TÉL. (1) 265 44 00 · 265 44 33 TÉLEX 260 300

Paris le 12 Octobre 1984

CONSEILS EN BREVETS D'INVENTION
MANDATAIRES EN BREVETS EUROPÉENS
EUROPEAN PATENT ATTORNEYS

RENÉ MARTINET
DOCTEUR EN DROIT
ANCIEN ELÈVE DE L'ECOLE POLYTECHNIQUE
INGENIEUR CIVIL DES TELECOMMUNICATIONS

ROLAND LAPOUX
DOCTEUR EN PHYSIQUE
DIPLÔME C.E.I.P.I.
DIPLÔME EN BREVETS D'INVENTION

OFFICE EUROPEEN DES BREVETS
Section de Dépôt
B.P 5818 Patentlaan 2
2280 RIJSWIJK (ZH)
PAYS BAS

RL/PS N° 13611

Re : Demande de brevet européen n° 84401597.4 du 30 Juillet 1984
au nom de l'Etablissement Public TELEDIFFUSION DE FRANCE
(invention de Alain R. CATREVAUX)

Messieurs,

Suite à votre demande de suppression de certaines irrégularités dans la demande de brevet européen identifiée ci-dessus, en date du 6 Septembre 1984, nous vous adressons une nouvelle description, de nouvelles revendications et de nouveaux dessins en trois exemplaires, conformes au règlement de la CBE.

Des corrections purement matérielles ont été apportées et sont les suivantes en référence à la description et aux revendications initialement déposées :

- page 1, ligne 6, lire -- Reed-Solomon -- ;
- page 1, ligne 10, remplacer "où" par -- ou -- ;
- page 3, ligne 18, lire -- Reed-Solomon -- ;
- page 9, ligne 10, remplacer "est" par -- sont -- ;
- page 12, ligne 15, remplacer "pose" par -- passe -- ;
- page 13, ligne 14, ajouter une parenthèse après "$(2^p)$" ;
- page 13, ligne 20, remplacer "18" par -- (18) -- ;
- page 13, ligne 21, remplacer "$Y_4\ Y_4^3$" par -- $Y_4\ X_4^3$ -- ;
- page 14, ligne 14, remplacer "$X_4^3$" par -- $X_4^2$ -- ;
- page 17, ligne 18, lire -- syndrome -- ;

- page 17, ligne 25, ajouter une virgule après "cas" ;
- page 21, revendication 1, lignes 1 et 2, lire -- Reed-Solomon -- ;
- page 22, lignes 14, 15 et 20 lire -- syndrome -- ;
- page 22, ligne 23, remplacer "15" par -- (15) -- ;
- dans la feuille d'abrégé, maintenant paginée 19, ligne 1, lire -- Reed-Solomon -- .

Veuillez agréer, Messieurs, l'expression de nos sentiments distingués et dévoués.

Roland LAPOUX

La requête en correction conforme à la R. 88 CBE est acceptée /à l'exception des points rayés/
LA HAYE, le 31.10.84
LA SECTION DE DEPOT

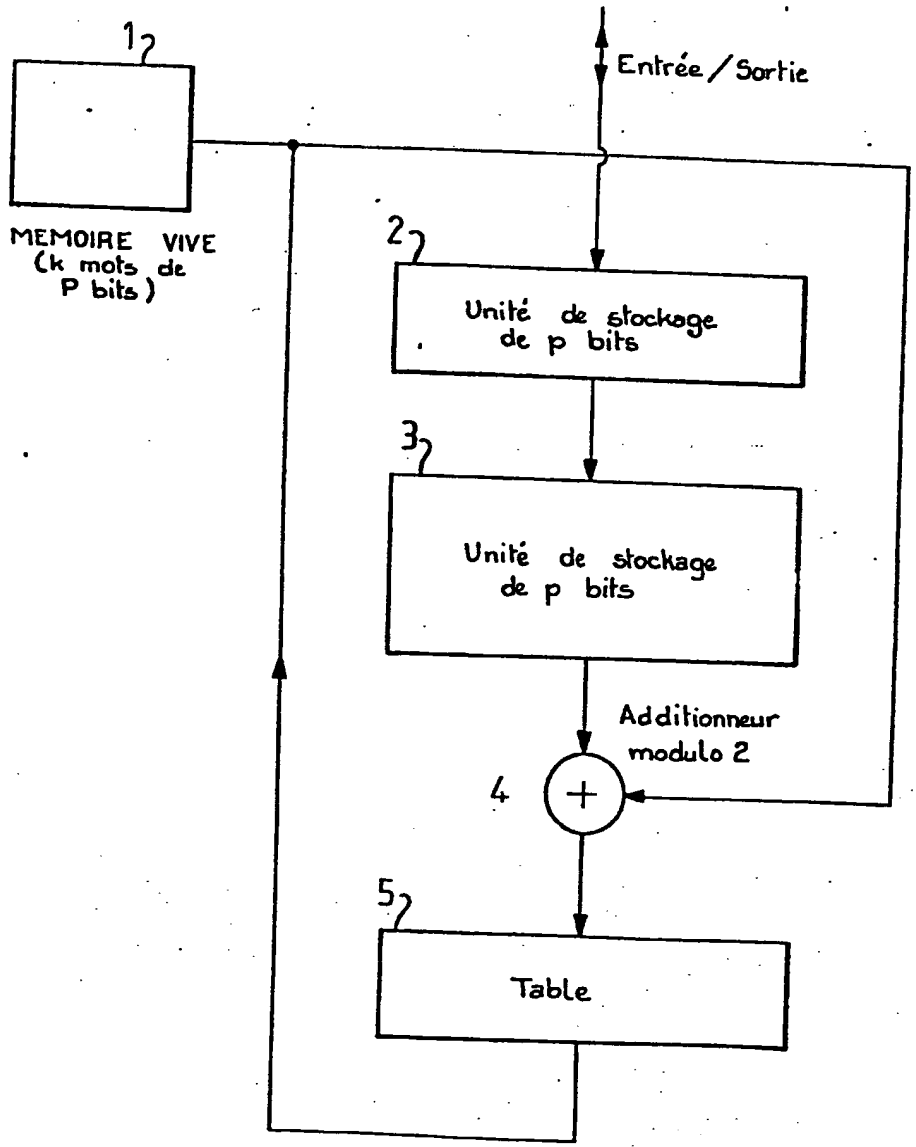

1
MEMOIRE VIVE
(k mots de
P bits)
Entrée / Sortie
2
Unité de stockage
de p bits
3
Unité de stockage
de p bits
Additionneur
modulo 2
4
5
Table

FIG-1

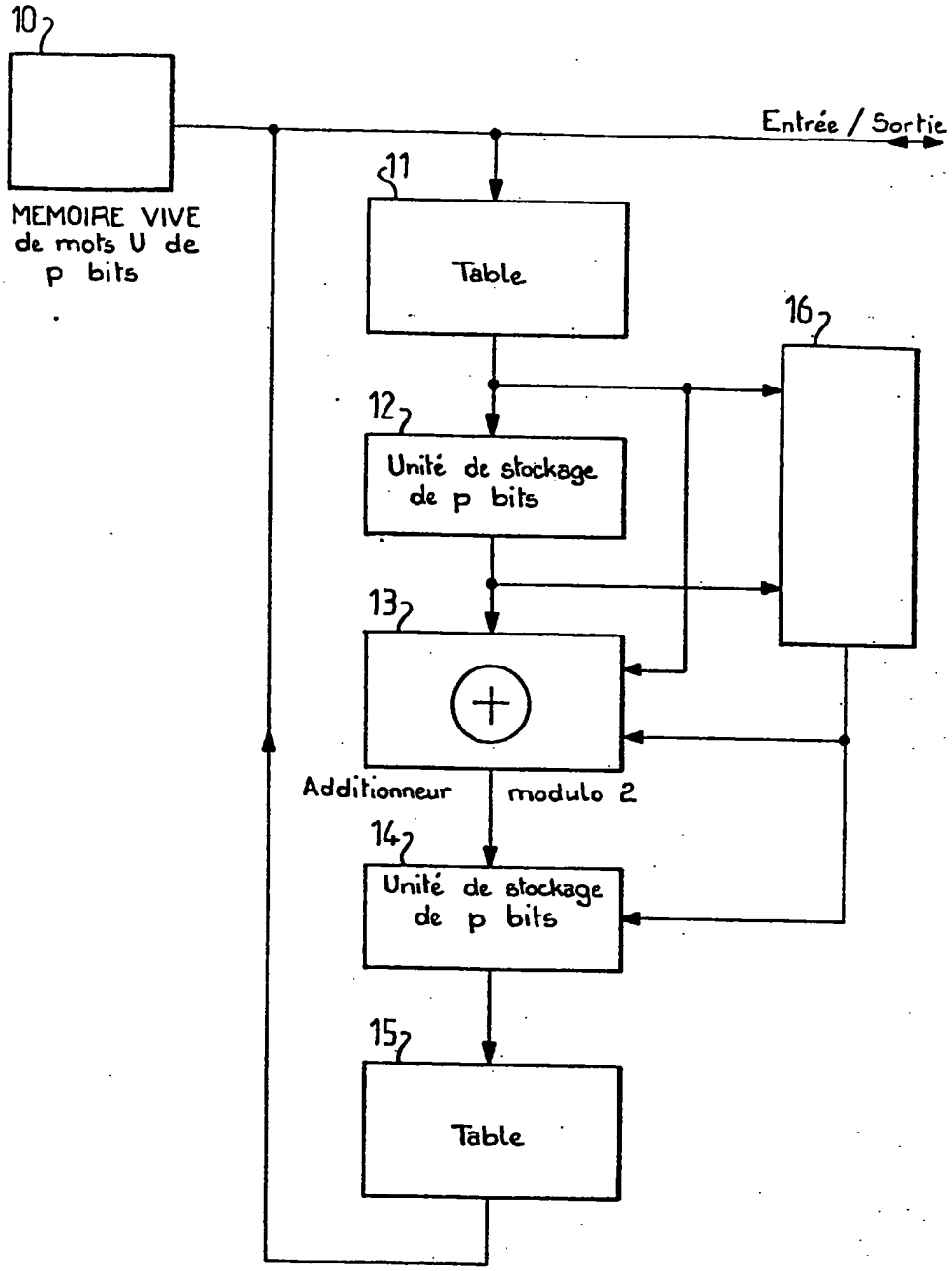
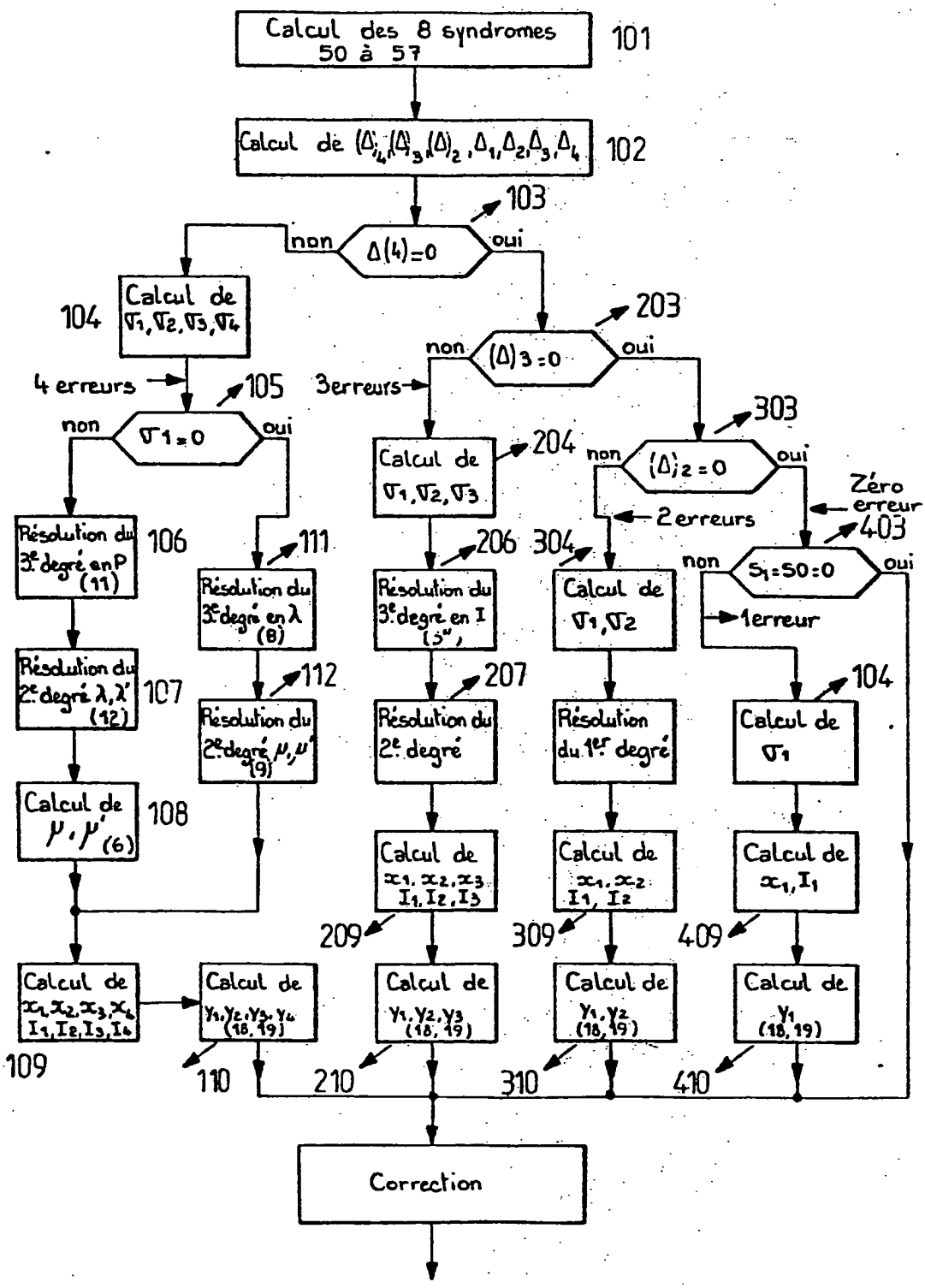

10
MEMOIRE VIVE de mots U de p bits
Entrée / Sortie
11
Table
16
12
Unité de stockage de p bits
13
Additionneur
modulo 2
14
Unité de stockage de p bits
15
Table

FIG 2

FIG-3


Calcul des 8 syndromes 50 à 57
101
Calcul de $(\Delta_4, (\Delta)_3, (\Delta)_2, \Delta_1, \Delta_2, \Delta_3, \Delta_4$
102
103
non
$\Delta(4)=0$
oui
104
Calcul de $\sigma_1, \sigma_2, \sigma_3, \sigma_4$
4 erreurs
105
non
$\sigma_1=0$
oui
203
non
$(\Delta)_3=0$
oui
3erreurs
303
Calcul de $\sigma_1, \sigma_2, \sigma_3$
204
non
$(\Delta)_2=0$
oui
Zéro erreur
403
2erreurs
Résolution du 3e degré en P (11)
106
111
Résolution du 3e degré en λ (8)
206
Résolution du 3e degré en I (5")
304
Calcul de $\sigma_1, \sigma_2$
non
$S_1=S_0=0$
oui
1erreur
Résolution du 2e degré λ, λ' (12)
107
112
Résolution du 2e degré μ, μ' (9)
207
Résolution du 2e degré
Résolution du 1er degré
104
Calcul de $\sigma_1$
Calcul de μ, μ' (6)
108
Calcul de $x_1, x_2, x_3$ $I_1, I_2, I_3$
209
Calcul de $x_1, x_2$ $I_1, I_2$
309
Calcul de $x_1, I_1$
409
Calcul de $x_1, x_2, x_3, x_4$ $I_1, I_2, I_3, I_4$
109
Calcul de $y_1, y_2, y_3, y_4$ (18, 19)
110
Calcul de $y_1, y_2, y_3$ (18, 19)
210
Calcul de $y_1, y_2$ (18, 19)
310
Calcul de $y_1$ (18, 19)
410
Correction

Office européen des brevets

# RAPPORT DE RECHERCHE EUROPEENNE

0133137
Numero de la demande

EP 84 40 1597

## DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie | Citation du document avec indication, en cas de besoin, des parties pertinentes | Revendication concernée | CLASSEMENT DE LA DEMANDE (Int. Cl.4) |
|---|---|---|---|
| A | SYSTEMS-COMPUTERS-CONTROLS, vol. 11, no. 6, novembre-décembre 1980, pages 58-67, Scripta Publishing Co., Silver Spring, Maryland, US; A. YAMAGISHI et al.: "A construction method for decoders of BCH codes using ROM's" * section 3, "Organization of decoder" * | 1-7 | H 03 M 13/00 |
| A | IEEE TRANSACTIONS ON COMPUTERS, vol. C-31, no. 2, février 1982, pages 170-175, IEEE, New York, US; K.Y. LIU: "Architecture for VLSI design of reed-solomon encoders" * section III: "Symbol-slice VLSI RS encoder architecture" | 1,6,7 | |
| A | EP-A-0 061 345 (SONY CORP.) * page 8, ligne 19 - page 13, ligne 4 * | 4-7 | DOMAINES TECHNIQUES RECHERCHES (Int. Cl.4) G 06 F 11/10 |
| A | IBM TECHNICAL DISCLOSURE BULLETIN, vol. 23, no. 10, mars 1981, pages 4597-4599, New York, US; C.L. CHEN: "Parallel implementation of double-error correction and triple-error detection" * page 4598, ligne 4 - page 4599, ligne 12 * | 5-7 | |

-/-

Le présent rapport de recherche a été établi pour toutes les revendications

| Lieu de la recherche | Date d'achèvement de la recherche | Examinateur |
|---|---|---|
| LA HAYE | 06-11-1984 | GUIVOL Y. |

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

OEB Form 1503. 03.82

Office européen des brevets

# RAPPORT DE RECHERCHE EUROPEENNE

EP 84 40 1597



## DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie | Citation du document avec indication, en cas de besoin, des parties pertinentes | Revendication concernée | CLASSEMENT DE LA DEMANDE (Int. Cl.4) |
|---|---|---|---|
| A | GB-A-2 093 238 (KOKUSAI DENSHIN DENWA)<br>* page 6, ligne 5 - page 8, ligne 2 * | 5-7 | |
| A | IBM TECHNICAL DISCLOSURE BULLETIN, vol. 18, no. 10, mars 1976, pages 3320-3321, New York, US; H.P. DUVOCHEL et al.: "Block check character determination in table look-up procedure"<br>* en entier * | 1-7 | DOMAINES TECHNIQUES RECHERCHES (Int. Cl.4) |

Le présent rapport de recherche a été établi pour toutes les revendications

| Lieu de la recherche | Date d'achèvement de la recherche | Examinateur |
|---|---|---|
| LA HAYE | 06-11-1984 | GUIVOL Y. |

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

OEB Form 1503 03 82